FIG. 1
(PRIOR ART)

PLAIN TEXT

IP — 110

L_0

R_0 — K_1

120

122 $\oplus$ 121 f

$L_1 = R_0$

$R_1 = L_0 \oplus f(R_0, K_1)$ — K_2

122 $\oplus$ 121 f

$L_2 = R_1$

$R_2 = L_1 \oplus f(R_1, K_2)$ — K_3

122 $\oplus$ 121 f

$L_3 = R_2$

$R_3 = L_2 \oplus f(R_2, K_3)$

$L_{14} = R_{13}$

$R_{14} = L_{13} \oplus f(R_{13}, K_{14})$ — K_{15}

122 $\oplus$ 121 f

$L_{15} = R_{14}$

$R_{15} = L_{14} \oplus f(R_{14}, K_{15})$ — K_{16}

122 $\oplus$ 121 f

$L_{16} = R_{15}$

$R_{16} = L_{15} \oplus f(R_{15}, K_{16})$

IP^{-1} — 130

CIPHER TEXT

FIG. 2
(PRIOR ART)

KEY

PC1 — 200

C_0 D_0

Left Shift — 220   Left Shift — 230

C_1 D_1

240 — PC2 → K_1

Left Shift — 220   Left Shift — 230

C_2 D_2

240 — PC2 → K_2

Left Shift — 220   Left Shift — 230

C_3 D_3

240 — PC2 → K_3

C_{14} D_{14}

240 — PC2 → K_{14}

Left Shift — 220   Left Shift — 230

C_{15} D_{15}

240 — PC2 → K_{15}

Left Shift — 220   Left Shift — 230

C_{16} D_{15}

240 — PC2 → K_{16}

FIG. 3
(PRIOR ART)

L(i−1)

R(i−1)

CIPHER FUNCTION

PC1 — 360

32

56

KEY

EXPANSION PERMUTATION UNIT — 310

PC2

48

390

320

48

48

Subkey(K$_I$)

S-Box

330

32

Shift — 370

Shift — 380

P-Box — 340

KEY SCHEDULER

32

32

350

L(i)

R(i)

KEY

S-Box Permutation

6-bit address

48-Bit Input

| S-Box 1 | S-Box 2 | S-Box 3 | S-Box 4 | S-Box 5 | S-Box 6 | S-Box 7 | S-Box 8 |

32-Bit Output

4-bit data

FIG. 4
(PRIOR ART)

IBR:
Input Buffer Register
64-bits (8-bytes)

OBR:
Output Buffer Register
64-bits (8-bytes)

Input Byte Stream

DES CORE

Output Byte Stream

FIFO

64-bit PlaiN Text →
64-bits Cipher Text

FIFO

Tinp

Tdes

Tout

8Clock Cycles

?

8Clock Cycles

P_i : i-th Plain Text I_i : i-th Input Processing
C_i : i-th Cipher Text D_i : i-th DES Processing
                                 O_i : i-th Output Processing

	P_0	P_1	P_2	•	P_{i-2}	P_{i-1}	P_i	•	•
Input Stage	I_0	I_1		•	•	•	I_i	•	•
DES Stage	–	D_0	D_1	D_2	•	•	D_{i-1}	•	•
Output Stage	–	–	O_0	O_1	O_2	•	O_{i-2}	•	•

T_p

$=\max(\text{Tinp}, \text{Tdes}, \text{Tout})$

C_0 C_1 C_2 • C_{i-2} C_{i-1} C_i

FIG. 5A
(PRIOR ART)

FIG. 5B

FIG. 6

Gather
Data
Formatting

Input Byte Stream

| I7 |
| I6 |
| I5 |
| I4 |
| I3 |
| I2 |
| I1 |
| I0 |

8Clock Cycles

• • •

CLK1 → IBR(L) ~610   CLK1 → IBR(R)
                                              ~620

32   32

Time Multiplexed Cipher Function

A_i 32   32 B_i

32   48   48
K_B K_A

632 ⊕ ← f_B f_A → ⊕ 635

32   631   634   32

CLK1 → A0 ~633   ~CLK1 → B0 ~636

32   32   32   32

32   32

~640   ~650

~CLK1 → OBR(L)   ~CLK1 → OBR(R)

Scatter
Data
Formatting

• • •

Output Byte Stream

| O7 |
| O6 |
| O5 |
| O4 |
| O3 |
| O2 |
| O1 |
| O0 |

8Clock Cycles

FIG. 7

A_i K_A B_i K_B

TIME MULTIPLEXED CIPHER FUNCTION

f_A f_B

A_i K_A B_i K_B

32   32

EXPANSION PERMUTATION UNIT — 710

EXPANSION PERMUTATION UNIT — 720

48   48   48   48

730 — ⊕   740 — ⊕

48   48

MULTIPLEXER — 750

48

S-Box PERMUTATION UNIT — 760

32

P-Box PERMUTATION UNIT — 770

32

Select — — — DE-MULTIPLEXER — 780

32   32

f_A f_B

FIG. 8

WHEN KEY IS LOADED FIRST TIME, IT SHOULD BE 1

Round	Left Shift Amount	Total Shift Amount
1(P_0)	3	1
2(P_1)	4	4
3(P_2)	4	8
4(P_3)	3	12
5(P_4)	4	15
6(P_5)	4	19
7(P_6)	4	23
8(P_7)	2	27

Round	Left Shift Amount	Total Shift Amount
1(Q_0)	4	2
2(Q_1)	4	6
3(Q_2)	4	10
4(Q_3)	3	14
5(Q_4)	4	17
6(Q_5)	4	21
7(Q_6)	3	25
8(Q_7)	2	0

Unit 1

Key — 56 — PC1 — 56 — 800

8 rounds — 28

C_A 710 — 28 — Left Shift 730 — 28

CLK1

PC2 750 — 48 — K_A

D_A 720 — 28 — Left Shift 740 — 28

8 rounds — 28

Unit 2

Key — 56 — PC1 — 56

8 rounds — 28

C_B — 28 — Left Shift — 28

~CLK1

PC2 — 48 — K_B

D_B — 28 — Left Shift 740 — 28

8 rounds — 28

FIG. 9

Timing labels (top): t0 t1 t2 t3 t4 t5 t6 t7 t8 t9 t10 t11 t12 t13 t14 t15 t16 t17 t18 t19

Periods (CLK1): P_0 P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_0 P_1

Periods (~CLK1): Q_0 Q_1 Q_2 Q_3 Q_4 Q_5 Q_6 Q_7 Q_0 Q_1

Signal										
CLK1										
~CLK1										
IN	I0	I1	I2	I3	I4	I5	I6	I7	I0	I1
IBR(L)	b_0	X	X	X	X	X	X	X	d_0	X
IBR(R)	a_0	X	X	X	X	X	X	X	c_0	X
f_A	b_1	b_3	b_5	b_7	b_9	b_{11}	b_{13}	b_{15}	d_1	d_3
f_B	b_2	b_4	b_6	b_8	b_{10}	b_{12}	b_{14}	b_{16}	d_2	d_4
K_A	K_1	K_3	K_5	K_7	K_9	K_{11}	K_{13}	K_{15}	K_1	K_3
K_B	K_2	K_4	K_6	K_8	K_{10}	K_{12}	K_{14}	K_{16}	K_2	K_4
A0	z_{16}	b_2	b_4	b_6	b_8	b_{10}	b_{12}	b_{14}	b_{16}	d_2
B0	z_{15} b_1	b_3	b_5	b_7	b_9	b_{11}	b_{13}	b_{15}	d_1	d_3
OBR(L)	–	z_{16}								b_{16}
OBR(R)	–	z_{15}								b_{15}
OUT	O7	O0	O1	O2	O3	O4	O5	O6	O7	O0

FIG. 10

t0 t1 t2 t3 t4 t5 t6 t7 t8 t9 t10 t11 t12 t13 t14 t15 t16 t17 t18 t19

P0 P1 P2 P3 P4 P5 P6 P7 P0 P1

CLK1

Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q0 Q1

~CLK1

| S_A | 3 | 4 | 4 | 3 | 4 | 4 | 4 | 2/1 | 3 | 4 |
| S_B | 2 | 4 | 4 | 4 | 3 | 4 | 4 | 3 | 2 | 4 | 4 |

| TS_A | 1 | 4 | 8 | 12 | 15 | 19 | 23 | 27 | 1 | 4 |
| TS_B | 0 | 2 | 6 | 10 | 14 | 17 | 21 | 25 | 0 | 2 | 6 |

| C_A, D_A | K_1 | K_3 | K_5 | K_7 | K_9 | K_{11} | K_{13} | K_{15} | K_1 | K_3 |
| C_B, D_B | K_{16} | K_2 | K_4 | K_6 | K_8 | K_{10} | K_{12} | K_{14} | K_{16} | K_2 | K_4 |

| K_A | K_1 | K_3 | K_5 | K_7 | K_9 | K_{11} | K_{13} | K_{15} | K_1 | K_3 |
| K_B | K_2 | K_4 | K_6 | K_8 | K_{10} | K_{12} | K_{14} | K_{16} | K_2 | K_4 |

FIG. 11

Input (Gather) with CK	Idle
16 Rounds DES Cos with CK	
Output (Scatter) with CK	Idle

8 Clock Cycles   8 Clock Cycles

16 Clock Cycles

Input (Gather) with CK
Micro-Pipelined DES Core with CK
Output (Scatter) with CK

8 Clock Cycles

FIG. 12